REMARKS

Claims 1-3, 7-11 and 17-21 were examined and reported in the Office Action. Claims 1-3, 7-11 and 17-21 are rejected. Claims 1, 7, 17 and 21 are amended. Claims 1-3, 7-11 and 17-21 remain.

Applicant requests reconsideration of the application in view of the following remarks.

I. 35 U.S.C. §112

It is asserted in the Office Action that claims 1-3, 7-11, and 17-21 are rejected under 35 U.S.C. §112 as failing to comply with the written description requirement. Applicant respectfully traverses the aforementioned rejection for the following reasons. Applicant notes that the specification asserts that each key is customized and distributed to an individual user. The plain meaning of the limitation of "assigned to" means to transfer or belongs to. This is clearly supported in the specification. As each individual user is distributed an individual customized key, each individual is therefore assigned a specific key. That is, each individual user has there own, specific and customized key. Applicant, however, has amended claims 1, 7 and 17 to include the limitations of "each of said plurality of individual keys is customized for a specific user."

Accordingly, withdrawal of the 35 U.S.C. § 1112, first paragraph rejections for claims 1-3, 7-11, and 17-21 is respectfully requested.

II. 35 U.S.C. §103

It is asserted in the Office Action that claim 21 is rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 5,956,407 issued to Slavin ("Slavin"), in view of U. S. Patent 5,933,501 issued to Leppek ("Leppek"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

According to MPEP §2142

> [t]o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." (In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Further, according to MPEP §2143.03, "[t]o establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. (In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)." "*All words in a claim must be considered* in judging the patentability of that claim against the prior art." (In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970), emphasis added.)

Applicant's amended claim 21 contains the limitations of

> distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another and each individual key is customized for a specific user; distribute a plurality of individual decryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another, and each different individual decryption process to decrypt an encrypted content differently from one another, and each individual decryption process is customized for a specific user; distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual encryption processes being different from one another, and each different individual encryption process to encrypt content differently from one another, and each individual encryption process is customized for a specific user.

That is, users each receive a different decryption process (i.e., different software executable code) for decrypting content encrypted with the main encryption process. Users also each have a different encryption process (i.e., different software executable code) for encrypting content to be decrypted with the main decryption process and the main key. Each of the differing decryption and encryption processes have distinct individual keys. Thus, each individual user is distributed an individual key, decryption process and encryption process customized for the specific user. Each decryption process decrypts an encrypted content differently from one another. For example, if a plurality of users wanted to download/receive the same content (e.g., a same video stream, a same audio stream, etc.), each user will have a different decryption process. Therefore, a user could not use their specific decryption process to decrypt the content that was sent/received by another user, even if the content is the same (because each is encrypted specifically for the specific user). Each encryption process encrypts content differently from one another. For example, if a plurality of users wanted to upload/transmit the same content (e.g., a same video stream, a same audio stream, etc.), each user will have a different encryption process (e.g., a different application program created for the specific user). This makes it harder for someone to be able to intercept content as the content that is uploaded/transmitted by each user would need to be decrypted differently.

Slavin discloses a method for encrypted communication where messages are created and public keys are looked up for a recipient. The message is encoded by a first process using a first portion of the public key to generate an intermediate encoded message. Then a second encoding process uses a second portion of the public key to generate the final encoded message. The final encoded message is sent to a recipient. "To decode the message, the receiver has created a decoding key as a function of the prime factors used to create the encoding key." (Slavin, column 6, lines 31-34). That is, each recipient uses the same decoding process and different decoding keys. Slavin discloses modifying the RSA technique disclosed by Rivest et al. (4,405,829).

Slavin discloses that E_m are public encoding keys. (Slavin, column 4, lines 15-20). Slavin does not teach, disclose or suggest the limitations in claim 21 of

> distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another and each individual key is customized for a specific user; distribute a plurality of individual decryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another, and each different individual decryption process to decrypt an encrypted content differently from one another, and each individual decryption process is customized for a specific user; distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual encryption processes being different from one another, and each different individual encryption process to encrypt content differently from one another, and each individual encryption process is customized for a specific user.

Leppek discloses a "virtual" encryption method that uses a sequence of encryptor operators to form a compound encryption operator. Leppek further discloses that "the data processing scheme of the present invention is effectively a `virtual` encryption and decryption scheme, as it does not actually perform any encrypting of the data, but rather assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence of successively different encryption operators." (Leppek, column 4, lines 48-59). Leppek simply uses decryption operators from a decryption operator database to decrypt the stream that was virtually encrypted with a sequence of encryptor operators. The decryption process and encryption process does not change. That is, operators change, but the same process encrypts/decrypts content. Leppek does not teach, disclose or suggest the limitations in claim 21

> distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another and each individual key is customized for a specific user; distribute a plurality of individual decryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another, and each different individual decryption process to decrypt an encrypted content differently from one another, and each individual decryption process is customized for a specific user; distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual encryption processes being different from one another, and each different individual encryption process to encrypt content differently from one another,

> and each individual encryption process is customized for a specific user.

Further, even if the disclosures of Slavin and Leppek were combined, the way each cryptographic system works are so different that the combined invention would teach away from each disclosure and the combined invention could not work.

Moreover, by viewing the disclosures of Slavin and Leppek, one can not jump to the conclusion of obviousness without impermissible hindsight. According to MPEP 2142,

> [t]o reach a proper determination under 35 U.S.C. 103, the examiner must step backward in time and into the shoes worn by the hypothetical 'person of ordinary skill in the art' when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention 'as a whole' would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the 'differences,' conduct the search and evaluate the 'subject matter as a whole' of the invention. The tendency to resort to 'hindsight' based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

Applicant submits that without first reviewing Applicant's disclosure, no thought, whatsoever, would have been made to generating individual customized decryption processes that are each different from one another and that decrypts encrypted content differently from one another, nor generating individual customized encryption processes that are each different from one another and that encrypts content differently from one another.

Therefore, neither Slavin, Leppek, and therefore, nor the combination of the two teach, disclose or suggest the limitations contained in Applicant's amended claim 21, as listed above. Since neither Slavin, Leppek, and therefore, nor the combination of the two teach, disclose or suggest all the limitations of Applicant's amended claim 21, Applicant's amended claim 21 is not obvious over Slavin in view of Leppek since a *prima facie* case of obviousness has not been met under MPEP §2142.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection for claim 21 is respectfully requested.

III. Claims Not Rejected Over Prior Art

Applicant notes that claims 1-3, 7-11 and 17-20 are not rejected over prior art. Applicant notes the arguments and amendments to claims 1, 7 and 17 overcome the 35 U.S.C. § 1112, first paragraph rejections and are fully supported by the original specification.

Applicant respectfully asserts that claims 1-3, 7-11 and 17-21, as they now stand, are allowable for the reasons given above.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely 1-3, 7-11 and 17-21, patentably define the subject invention over the prior art of record and are in condition for allowance and such action is earnestly solicited at the earliest possible date.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: September 12, 2006

By: _____
Steven Laut, Reg. No. 47,736

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail with sufficient postage in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia 22313-1450 on September 12, 2006.

_____
Jean Svoboda